News & Analysis

NSA keys into quantum computing

Leaked documents suggest that the US National Security Agency is developing quantum computers to crack cryptography codes, but what progress has the agency really made? **Jon Cartwright** investigates

The US National Security Agency (NSA) has a classified programme to build a quantum computer that can break modern Internet security, according to documents leaked by the former NSA contractor Edward Snowden. The documents, which were published last month in redacted form by the *Washington Post*, have surprised few physicists working in the field. However, they have led to speculation about the status of NSA research and a renewed debate on the risks of developing quantum computers.

Quantum computers are devices that rely on quantum phenomena such as superposition, in which a system exists in multiple states at once, and entanglement, in which the states of two systems become inextricably linked. Unlike classical computers, which store bits of information in definite values of 0 or 1, quantum computers store information in quantum bits, or qubits, which are a superposition of both. When qubits are entangled, any change in one immediately effects changes in the others. Qubits can therefore work in unison and solve certain complex problems much faster than their classical counterparts.

Some of these problems are purely scientific in nature, such as simulating molecules inside biological cells, which could allow researchers to develop more effective drugs. But one problem quantum computers are expected to be most proficient at is factorizing large numbers. If successful, this would allow supposedly secure information on the Internet to be deciphered, including banking transactions, private messages and government files. Although in principle classical computers could perform the same deciphering, the process would usually take so long as to be unfeasible.

In 2006 the NSA openly announced the creation of a joint institute with the University of Maryland in College Park and the National Institute of Standards and Technology in Gaithersburg, both in the US, to develop quantum technology, including quantum computing. But the new documents reveal an additional classified effort at Maryland with the express purpose of breaking data encryption. They state that the NSA wants to build "a cryptologically useful quantum computer" as part of a programme titled "Penetrating Hard Targets", which the *Post* claims has a budget of $79.7m (£48m).

NSA

Listening in
The US National Security Agency is allegedly developing quantum computers with the aim of breaking quantum cryptography codes.

Many physicists working in the field of quantum information believe quantum computing is exactly the sort of technology one would expect the NSA to develop. "If you put my level of surprise on a scale from zero to 10, where 10 is very, very surprised, my answer would be zero," says Raymond Laflamme, a leading quantum-information theorist who is based at the University of Waterloo in Canada. "If they were not doing it, they would not be doing their job." Even so, the news has confirmed for many others how important it is to find other ways to make digital information secure.

Unbreakable codes?

Encrypted information on the Internet exists on pages whose URL begins with "https://" as opposed to "http://". It is based on public-key cryptography, which allows someone to send information to someone else by encoding it with a publicly available key. Although anyone on the Internet could intercept and read the message in its encrypted form, only the receiver, who holds a special, private key, can decipher it.

The most common type of public-key encryption is RSA, which was invented by the cryptographers Ron Rivest, Adi Shamir and Len Adleman in the late 1970s. In RSA encryption, both the public and private keys are derived from a pair of large prime numbers, the product of which anyone can find out. If you know the formula, you can in theory work backwards, factorizing the product until you discover the primes – but it is only realistically solvable if your computer is powerful enough.

Quantum computers could do that kind of factorization – and as Laflamme points out, it does not matter that they have not been properly realized yet. Information on the Internet can easily be stored, which indeed the NSA – as well as the UK Government Communications Headquarters (GCHQ), other intelligence agencies and private cloud-computing companies – is doing routinely anyway. That means information encrypted today could be deciphered in 10 years' time – or whenever quantum computers are finally in use.

How much of a problem that poses depends on the sort of information you are encrypting, explains Laflamme, who gives the example of someone using a computer to buy something with a credit card. The development of a quantum computer is not a threat because in 10 years you will have changed your credit card, and unless you are buying something illegal, you will not care that the NSA knows. "But what if you're sending the explanation of a new type of classified technology, one you want to keep secret for 20 years?" asks Laflamme. "Well, then it's problematic."

There are methods to future-proof the transfer of secret information.

One is to create a communication network independent of the Internet through which users can share secret keys, which can then be used to encrypt and decipher messages on the Internet. The security of such networks can be improved further with quantum key distribution (QKD), which in theory guarantees the security of the key transfer – although the latest documents also reveal that the NSA is attempting to exploit practical loopholes in this, too, under a programme known as "Owning the Net".

Vadim Makarov, who himself studies flaws in practical QKD systems at the University of Waterloo, says that cryptographers are also looking into classical "quantum-safe" encryption algorithms for use on the Internet. Like quantum computing, however, quantum-safe encryption and foolproof QKD systems, which cannot be cracked at all, are also taking time to develop and implement. "I just hope we won't be too late," he says.

Secret race

The NSA has not publicly responded to the leaks, but another question raised by the NSA documents is whether the agency could be further ahead in the development of quantum computing than major labs. The main reason functional quantum computers are expected to be many years away is that it is still very difficult to control qubits while protecting them from external interference that can all too easily destroy them. Moreover, no-one is yet sure what type of qubits are most likely to be practical, with physicists exploring types made from trapped ions, photons and superconducting circuits, to name but three.

According to the documents, the NSA expected its scientists to have demonstrated "dynamical decoupling and complete quantum control on two semiconductor qubits" by the end of September 2013. Purely on numbers, the agency would appear to be lagging behind major labs such as the Institute for Experimental Physics at the University of Innsbruck in Austria, which demonstrated entanglement of 14 atomic qubits as far back as 2010. On the other hand, control of qubits made of the semiconductor silicon is less advanced, with only single silicon qubits having been openly demonstrated since 2012. If the NSA has already succeeded in achieving control of two silicon qubits, then it may be ahead in that particular race.

The semiconductor mentioned in the documents could also refer to types of semiconductor that turn superconducting in certain regimes. But experimental quantum physicist Jonathan Home of ETH Zurich in Switzerland believes the NSA is indeed pursuing a regular semiconductor such as silicon, because the "dynamical decoupling" also mentioned – a type of noise mitigation – is not usually applied to superconducting qubits. If the agency is pursuing silicon, that might be because it is easy to build large arrays of silicon devices, Home says. But he adds that it is not so easy with silicon to implement the error correction that would make any devices function like proper qubits. "If I were an NSA manager, maybe I know the solid-state can be scaled up, so I pick that. But maybe I haven't thought so hard about actual quantum computing," he says.

It is still very difficult to control qubits while protecting them from external interference that can all too easily destroy them

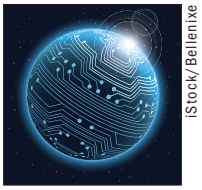
If the NSA is developing quantum computers, does that mean that other intelligence agencies such as GCHQ are too? Physicists contacted by *Physics World* were not sure whether an agency outside the US would have the resources. But one point is obvious: over every development in quantum computing in the coming years, the spies will be watching.

Innovation

UK splashes out £270m on quantum technology

Further details have emerged of a new £270m initiative being funded by the UK government to convert quantum-physics research into commercial products. The five-year initiative, which will include the creation of a network of quantum-technology centres, was one of a number of measures revealed by the government in its Autumn Statement in early December 2013 to boost the UK's science base. The chancellor George Osborne said that the money was "additional investment" in research and that science was a "personal priority" of his.

The initiative, which will begin in 2015, will focus on areas such as chip-scale atomic clocks for improved GPS communication, quantum-enabled sensors, quantum communication and quantum computing. Some cash will go to existing university research groups, while about £30m per year will go to the Technology Strategy Board – the UK's national innovation agency – to support immediate commercialization of technology. There will also be money for PhD students and postdocs, while some £4m will go on equipment for the new Advanced Metrology Laboratory being built at the National Physical Laboratory.



iStock/Bellenixe

Quantum commerce The UK has announced it will establish a network of quantum-technology centres to convert quantum-physics research into commercial products.

The quantum-physics initiative, which has involved careful behind-the-scenes negotiations between the UK physics community, government and industry, was formally put to Osborne last year by a group of physicists led by Peter Knight from Imperial College London. Knight, who is the immediate past president of the Institute of Physics, which publishes *Physics World*, says that the prospect of an extra £270m for quantum technology is "highly exciting". However, he adds that he will be "keeping a close eye" to ensure the cash is not simply siphoned off from budgets earmarked for other scientific fields.

The detailed mechanism for distributing the funding among UK researchers is still being discussed, although it is likely to involve the UK's research councils, the Royal Society and the Royal Academy of Engineering. However, Jeremy O'Brien from the University of Bristol, who also helped to get the initiative off the ground, says the UK must properly co-ordinate the new investment. "Fragmentation into small chunks will be the enemy of progress and ultimately could hinder the creation of wealth," he says.

But participants are optimistic about what the initiative can achieve. "There is real potential for long-term transformational change in some information-related technologies, deriving from a complete re-conception of design principles underpinning their operation," says Ian Walmsley from the University of Oxford.

Matin Durrani